AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Union Calendar No. 292

109TH CONGRESS
2D SESSION

H. R. 5318

[Report No. 109–522]

To amend title 18, United States Code, to better assure cyber-security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 9, 2006

Mr. SENSENBRENNER (for himself, Mr. COBLE, Mr. SMITH of Texas, Mr. FEENEY, Mr. SCHIFF, and Ms. PRYCE of Ohio) introduced the following bill; which was referred to the Committee on the Judiciary

JUNE 22, 2006

Additional sponsor: Mr. CHABOT

JUNE 22, 2006

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on May 9, 2006]

A BILL

To amend title 18, United States Code, to better assure cyber-security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006".

SEC. 2. PERSONAL ELECTRONIC RECORDS.

Section 1030(a)(2) of title 18, United States Code, is amended—

(1) by striking "or" at the end of subparagraph (B); and

(2) by adding at the end the following:

"(D) a means of identification (as defined in section 1028(d)) from a protected computer; or

"(E) the capability to gain access to or remotely control a protected computer.".

SEC. 3. USE OF FULL INTERSTATE AND FOREIGN COMMERCE POWER FOR CRIMINAL PENALTIES.

(a) BROADENING OF SCOPE.—Section 1030(e)(2)(B) of title 18, United States Code, is amended by inserting "or affecting" after "which is used in".

(b) ELIMINATION OF REQUIREMENT OF AN INTERSTATE OR FOREIGN COMMUNICATION FOR CERTAIN OFFENSES INVOLVING PROTECTED COMPUTERS.—Section 1030(a)(2)(C) of title 18, United States Code, is amended by striking "if the conduct involved an interstate or foreign communication".

SEC. 4. RICO PREDICATES.

Section 1961(1)(B) of title 18, United States Code, is amended by inserting "section 1030 (relating to fraud and related activity in connection with computers)," before "section 1084".

SEC. 5. CYBER-EXTORTION.

Section 1030(a)(7) of title 18, United States Code, is amended by inserting ", or to access without authorization or exceed authorized access to a protected computer" after "cause damage to a protected computer".

SEC. 6. CONSPIRACY TO COMMIT CYBER-CRIMES.

Section 1030(b) of title 18, United States Code, is amended by inserting "or conspires" after "attempts".

SEC. 7. NOTICE TO LAW ENFORCEMENT.

(a) CRIMINAL PENALTY FOR FAILURE TO NOTIFY LAW ENFORCEMENT.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"§ 1039. Concealment of security breaches involving personal information

"(a) OFFENSE.—Whoever owns or possesses data in electronic form containing a means of identification (as defined in section 1028), having knowledge of a major security breach of the system containing such data maintained by such person, and knowingly fails to provide notice of such breach to the United States Secret Service or Federal Bureau of Investigation, with the intent to prevent, obstruct,

or impede a lawful investigation of such breach, shall be fined under this title, imprisoned not more than 5 years, or both.

"(b) DEFINITIONS.—As used in this section—

"(1) MAJOR SECURITY BREACH.—The term 'major security breach' means any security breach—

"(A) whereby means of identification pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired, and such acquisition causes a significant risk of identity theft;

"(B) involving databases owned by the Federal Government; or

"(C) involving primarily data in electronic form containing means of identification of Federal Government employees or contractors involved in national security matters or law enforcement.

"(2) SIGNIFICANT RISK OF IDENTITY THEFT.—

"(A) IN GENERAL.—The term 'significant risk of identity theft' means such risk that a reasonable person would conclude, after a reasonable opportunity to investigate, that it is more probable than not that identity theft has occurred or will occur as a result of the breach.

"(B) PRESUMPTION.—If the data in electronic form containing a means of identification involved in a suspected breach has been encrypted, redacted, requires technology to use or access the data that is not commercially available, or has otherwise been rendered unusable, then there shall be a presumption that the breach has not caused a significant risk of identity theft. Such presumption may be rebutted by facts demonstrating that the encryption code has been or is reasonably likely to be compromised, that the entity that acquired the data is believed to possess the technology to access it, or the owner or possessor of the data is or reasonably should be aware of an unusual pattern of misuse of the data that indicates fraud or identity theft.".

(b) RULEMAKING.—Within 180 days after the date of enactment of this Act, the Attorney General and Secretary of Homeland Security shall jointly promulgate rules and regulations, after adequate notice and an opportunity for comment, as are reasonably necessary, governing the form, content, and timing of the notices required pursuant to section 1039 of title 18, United States Code. Such rules and regulations shall not require the deployment or use of specific products or technologies, including any specific com-

puter hardware or software, to protect against a security breach. Such rules and regulations shall require that—

(1) such notice be provided to the United States Secret Service or Federal Bureau of Investigation before any notice of a breach is made to consumers under State or Federal law, and within 14 days of discovery of the breach;

(2) if the United States Secret Service or Federal Bureau of Investigation determines that any notice required to be made to consumers under State or Federal law would impede or compromise a criminal investigation or national security, the United States Secret Service or Federal Bureau of Investigation shall direct in writing within 7 days that such notice shall be delayed for 30 days, or until the United States Secret Service or Federal Bureau of Investigation determines that such notice will not impede or compromise a criminal investigation or national security;

(3) the United States Secret Service shall notify the Federal Bureau of Investigation, if the United States Secret Service determines that such breach may involve espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section

11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y))), except for offenses affecting the duties of the United States Secret Service under section 3056(a) of title 18, United States Code; and

(4) the United States Secret Service or Federal Bureau of Investigation notify the Attorney General in each State affected by the breach, if the United States Secret Service or Federal Bureau of Investigation declines to pursue a criminal investigation, or as deemed necessary and appropriate.

(c) IMMUNITY FROM LAWSUIT.—No cause of action shall lie in any court against any law enforcement entity or any person who notifies law enforcement of a security breach pursuant to this section for any penalty, prohibition, or damages relating to the delay of notification for law enforcement purposes under this Act.

(d) CIVIL PENALTY FOR FAILURE TO NOTIFY.—Whoever knowingly fails to give a notice required under section 1039 of title 18, United States Code, shall be subject to a civil penalty of not more than $50,000 for each day of such failure, but not more than $1,000,000.

(e) RELATION TO STATE LAWS.—

(1) IN GENERAL.—The requirement to notify law enforcement under this section shall supersede any

other notice to law enforcement required under State law.

(2) EXCEPTION FOR STATE CONSUMER NOTICE LAWS.—The notice required to law enforcement under this section shall be in addition to any notice to consumers required under State or Federal law following the discovery of a security breach. Nothing in this section annuls, alters, affects or exempts any person from complying with the laws of any State with respect to notice to consumers of a security breach, except as provided by subsections (b) and (c).

(f) DUTY OF FEDERAL AGENCIES AND DEPARTMENTS.—An agency or department of the Federal Government which would be required to give notice of a major security breach under section 1039 of title 18, United States Code, if that agency or department were a person, shall notify the United States Secret Service or Federal Bureau of Investigation of the breach in the same time and manner as a person subject to that section. The rulemaking authority under subsection (b) shall include the authority to make rules for notice under this subsection of a major security breach.

(g) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 47 of title 18, United States Code, is amended by adding at the end the following new item:

"1039. Concealment of security breaches involving personal information.".

SEC. 8. PENALTIES FOR SECTION 1030 VIOLATIONS.

Subsection (c) of section 1030 of title 18, United States Code, is amended to read as follows:

"(c)(1) The punishment for an offense under subsection (a) or (b) is a fine under this title or imprisonment for not more than 30 years, or both.

"(2) The court, in imposing sentence for an offense under subsection (a) or (b), shall, in addition to any other sentence imposed and irrespective of any provision of State law, order that the person forfeit to the United States—

"(A) the person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

"(B) any property, real or personal, constituting or derived from, any proceeds the person obtained, directly or indirectly, as a result of such violation.".

SEC. 9. DIRECTIVE TO SENTENCING COMMISSION.

(a) DIRECTIVE.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall forthwith review its guidelines and policy statements applicable to persons convicted of offenses under sections 1028, 1028A, 1030, 1030A, 2511 and 2701 of title 18, United States Code and any other relevant provisions of law, in order to reflect the intent of Congress that such

penalties be increased in comparison to those currently provided by such guidelines and policy statements.

(b) REQUIREMENTS.—In determining its guidelines and policy statements on the appropriate sentence for the crimes enumerated in paragraph (a), the Commission shall consider the extent to which the guidelines and policy statements may or may not account for the following factors in order to create an effective deterrent to computer crime and the theft or misuse of personally identifiable data—

(1) the level of sophistication and planning involved in such offense;

(2) whether such offense was committed for purpose of commercial advantage or private financial benefit;

(3) the potential and actual loss resulting from the offense;

(4) whether the defendant acted with intent to cause either physical or property harm in committing the offense;

(5) the extent to which the offense violated the privacy rights of individuals;

(6) the effect of the offense upon the operations of a government agency of the United States, or of a State or local government;

(7) whether the offense involved a computer used by the government in furtherance of national defense, national security or the administration of justice;

(8) whether the offense was intended to, or had the effect of significantly interfering with or disrupting a critical infrastructure;

(9) whether the offense was intended to, or had the effect of creating a threat to public health or safety, injury to any person, or death; and

(10) whether the defendant purposefully involved a juvenile in the commission of the offense to avoid punishment.

(c) ADDITIONAL REQUIREMENTS.—In carrying out this section, the Commission shall—

(1) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(2) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(3) make any conforming changes to the sentencing guidelines; and

(4) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

SEC. 10. DAMAGE TO PROTECTED COMPUTERS.

(a) Section 1030(a)(5)(B) of title 18, United States Code, is amended—

(1) by striking "or" at the end of clause (iv);

(2) by inserting "or" at the end of clause (v); and

(3) by adding at the end the following:

"(vi) damage affecting ten or more protected computers during any 1-year period.".

(b) Section 1030(g) of title 18, United States Code, is amended by striking "or" after "(iv)," and inserting ", or (vi)" after "(v)".

(c) Section 2332b(g)(5)(B)(i) of title 18, United States Code, is amended by striking "(v) (relating to protection of computers)" and inserting "(vi) (relating to the protection of computers)".

SEC. 11. ADDITIONAL FUNDING FOR RESOURCES TO INVESTIGATE AND PROSECUTE CRIMINAL ACTIVITY INVOLVING COMPUTERS.

(a) ADDITIONAL FUNDING FOR RESOURCES.—

(1) AUTHORIZATION.—In addition to amounts otherwise authorized for resources to investigate and prosecute criminal activity involving computers, there are authorized to be appropriated for each of the fiscal years 2007 through 2011—

(A) $10,000,000 to the Director of the United States Secret Service;

(B) $10,000,000 to the Attorney General for the Criminal Division of the Department of Justice; and

(C) $10,000,000 to the Director of the Federal Bureau of Investigation.

(2) AVAILABILITY.—Any amounts appropriated under paragraph (1) shall remain available until expended.

(b) USE OF ADDITIONAL FUNDING.—Funds made available under subsection (a) shall be used by the Director of the United States Secret Service, the Director of the Federal Bureau of Investigation, and the Attorney General, for the United States Secret Service, the Federal Bureau of Investigation, and the criminal division of the Department of Justice, respectively, to—

(1) hire and train law enforcement officers to—

(A) investigate crimes committed through the use of computers and other information technology, including through the use of the Internet; and

(B) assist in the prosecution of such crimes; and

(2) procure advanced tools of forensic science to investigate, prosecute, and study such crimes.

Union Calendar No. 292

109TH CONGRESS
2D SESSION

H. R. 5318

[Report No. 109–522]

A BILL

To amend title 18, United States Code, to better assure cyber-security, and for other purposes.

JUNE 22, 2006

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed